IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	**CRIMINAL NO. 2:16cr104**
	)	
LARRY JAMES REECE II,	)	
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE TO DEFENDANT'S FIRST MOTION TO SUPPRESS

Now comes the United States of America, by and through attorneys, Dana J. Boente, United States Attorney for the Eastern District of Virginia, and Elizabeth M. Yusi, Assistant United States Attorney, and submits its response in opposition to the defendant, LARRY JAMES REECE II's First Motion to Suppress the search warrant of his residence. For the reasons set forth below, the defendant's motion should be denied.

INTRODUCTION

In September 2015, the Homeland Security Investigations (HSI) Cyber Crimes Center, Child Exploitation Investigations Unit (C3/CEIU) became involved in an ongoing child pornography investigation. This investigation involved multiple individuals, believed to be residing across the United States as well as abroad, who are members of an Internet-based

bulletin board[1] (hereafter referred to as Bulletin Board A) dedicated to the advertisement, distribution and production of child pornography. Bulletin Board A had over 1,500 "approved users[2]," who actively posted new content and engaged in online discussions involving the sexual exploitation of minors. In general, members would post preview images and download links to several different cloud-based storage services[3]. Among other things, these posts contained the

[1] "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the Website Administrator.

[2] This figure is taken from a posting by one of Bulletin Board A's administrators. Administrators manage the technical details required for the running of the site. As such, they may promote members, set rules, create sections and act as moderators.

[3] "Cloud-based storage service," as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an Internet connection.

title of the image, the file name, the file size, and a password[4] which users could input to access and open the content of the file associated with the image file. Law enforcement obtained a court order under 18 U.S.C. § 2703(d) from the United States District Court for the District of Columbia to one of the cloud-based storage services concerning the unique download links found on Bulletin Board A. The storage service provided, among other information, business records that contained the IP addresses connected to the downloading of the specific files. The users connected to the IP addresses actually attempted, if not succeeded, in downloading the information. Among the IP addresses identified accessing Bulletin Board A was one associated with defendant LARRY JAMES REECE II. Following the execution of a search warrant at REECE's home in Chesapeake, Virginia, REECE was indicted and arrested on charges of receipt and access with intent to view child pornography involving a prepubescent minor. REECE now seeks to suppress the information obtained by the search warrant of his home. For the reasons that follow, his motion should be denied.

First, the affidavit supporting the search warrant application for REECE's residence set forth ample probable cause to conclude that any user downloading the child pornography from the cloud-based service may have evidence of child pornography at the residence connected to the Internet account. Any user of Bulletin Board A knew of its illicit content and intended to access that content. Bulletin Board A was no ordinary website, but a hidden service operating on an anonymous network that was dedicated to the sharing of child pornography. The

[4] Defendant claims that the affiant to the application "omits the fact that the person using Mr. Reece's IP address never entered a password to access the video." Def. Mot. at 4 (emphasis omitted). However, without having access to the user's computer prior to the search warrant, the government is unaware how the affiant could know such information.

magistrate judge who authorized the warrant reasonably concluded that there was a fair probability that anyone who logged into the cloud-based storage service links did so with knowledge of its content and intent to view that content.

Second, the defendant's claim that the probable cause supporting the search warrant was stale has no merit. Looking at the totality of the circumstances, the five-month delay between the criminal activity and the search warrant did not make the probable cause stale. Especially considering the Fourth Circuit has stated that child pornography activity is not stale as a matter of law if acted upon within a year.

Third, the defendant makes no showing—much less a substantial, preliminary one—to justify a *Franks* hearing. Everything is the affidavit was and remains accurate. REECE cannot and does not point to anything that was not true or that was omitted. Defendant's *Franks* arguments consist of little more than a disagreement with the opinions and conclusions of the veteran HSI agent contained within his affidavit, none of which suffice to justify a *Franks* hearing.

Finally, even if the search warrant was somehow flawed, the good faith exception is an independent bar to suppression. The warrant affidavit set forth probable cause for its request to search a particular location for particular information. And, a neutral and detached magistrate relied on that affidavit in authorizing the warrant. Law enforcement's reliance on that authorization was therefore objectively reasonable and suppression is thus unwarranted.

For these and the other reasons outlined below, the defendant's first motion to suppress should be denied.

BACKGROUND

The charges in this case arise from an investigation into Bulletin Board A, a global online forum through which users advertised, distributed, and/or accessed illegal child pornography. Images and videos shared through the site were highly categorized according to victim age and gender, as well as the type of sexual activity. The site also included forums for discussion of all things related to child sexual exploitation, including tips for grooming victims and avoiding detection.

I. The Network

Bulletin Board A operated on a network ("the Network[5]") available to Internet users who were aware of its existence. The Network was designed specifically to facilitate anonymous communication over the Internet. In order to access the Network, a user must have installed computer software that is publicly available, either by downloading software to the user's existing web browser, downloading free software available from the Network's administrators, or downloading a publicly-available third-party application.[6] Using the Network prevented someone attempting to monitor an Internet connection from learning what sites a user visited and

[5] The actual name of the Network is known to law enforcement. The network remains active and disclosure of the name of the network would potentially alert its members to the fact that law enforcement action is being taken against the network, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the network will be identified as "the Network."

[6] Users may also access the Network through so-called "gateways" on the open Internet, however, use of those gateways does not provide users with the full anonymizing benefits of the Network.

prevented the sites the user visited from learning the user's physical location. The Network's software protected users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user. Because of the way the Network routed communication through other computers, traditional IP identification techniques were generally not viable.

Websites that were accessible only to users operating within the Network can be set up within the Network. Bulletin Board A was one such website. These websites operated the same as regular public websites with one critical exception - the IP address for the web server was hidden and instead was replaced with a Network-based web address. A user could only reach such sites if the user was using the Network client and operating in the Network. In order to access Bulletin Board A, a user also had to either know the exact web address or discover its exact web address, for example, from other users or from servers on the Network that maintain indexes of known servers. Moreover, because neither a user nor law enforcement could identify the actual IP address of the web server, it was not possible to determine through public lookups where the computer that hosts the website was located. Accordingly, it was not possible to obtain data detailing the activities of the users from the website server through public lookups.

II. Bulletin Board A and its contents.

Bulletin Board A was dedicated to the advertisement and distribution of child pornography. It had over 1,500 users who actively posted new content and who engaged in online discussions involving the sexual exploitation of minors. Bulletin Board A had various

sections containing forums and subforums in which members posted messages and/or images for other members to view. For example, there were sections labeled "Girls" and "Boys" and within each of these sections are several forums, including: "Pre-teen Hardcore;" "Pre-teen Softcore/Non-nude;" "Model/Producer section;" "Babies and toddlers" and "Requests." Typical posts contained: text; preview images of child pornography or erotica available for download; links to external file sharing websites from which the advertised images or videos may be downloaded; and any required passwords.

Although Bulletin Board A itself operated on the anonymity network described herein, many of the external file sharing websites from which images or videos advertised on Bulletin Board A would be downloaded operated on the ordinary Internet. The investigation determined that some users accessed and downloaded child pornography images and videos advertised on Bulletin Board A from those file sharing sites without using the anonymity network. Accordingly, IP address information was available to help identify such users.

In October of 2015, C3/CEIU began working with the Department of Justice, Child Exploitation and Obscenity Section (CEOS), High Technology Investigative Unit (HTIU). Since that time, HTIU has captured content contained on and advertised through Bulletin Board A. C3/CEIU personnel reviewed this content and observed various postings by board members. One such post was found within the section titled "Girls," forum "Pre-teen Hardcore," sub-forum "Videos." This post was made to the board by a member (hereafter referred to as Board Member A) on October 26, 2015, and it consisted of the title: "Hot latin doggyfuck" followed by a preview still image file containing several smaller still images from the video in question, affording the user the opportunity to pre-view the content of said video. In addition, the posting

provided the filename: "(~pthc center~)(opva)(2013) Hot latin doggyfucking WP_20130324_052315Z," the file size: 7.70 MB, the Archive name: myuimy5r6yu5e433e.7z, the Duration: 00:00:49, the Download link, Password, and the Download key, among other information. If the user were to hover their cursor over the download link, the post would provide the full download link: http://[FSS].com/mkj6j8qjxixb/myuimy5r6yu5e433e.7z.html.[7] This post also contained a password, which users could input to open the content of the file associated with that unique URL[8].

HTIU downloaded the file titled "(~pthc center~)(opva)(2013) Hot latin doggyfucking WP_20130324_052315Z" from the above listed URL. This file was encrypted, but by using the password provided in the post detailed above, the file could be opened and viewed. The video file consisted of what appeared to be an adult male engaged in sexual activity with what appeared to be an underage minor. Specifically, the video depicted a scene recorded from above, showing what appears to be an adult male from the waist down, with his pants pulled

[7] The unique string of characters in this file path following the words [FSS].com is known to law enforcement. Disclosure of the unique string of characters, or of the file-sharing service's name, could potentially alert investigation targets to the fact that law enforcement action is being taken against the board and its users, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, information from the unique URL has been replaced with generic characters and the file sharing service will be referred to generically as "FSS."

[8] The term URL (short for Universal Resource Locator) refers to the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies the specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

down and with an erect penis, and the lower back and buttocks of what appears to be a minor, engaging in sexual intercourse (either actual or simulated) until the adult male ejaculates on the apparent minor's back and buttocks. The video file is 49 seconds in duration and contains audio.

Law enforcement determined that these unique URLs, like the one mentioned above, that were posted by members of Bulletin Board A and which provided board members access to files depicting minors engaging in sexually explicit conduct, were hosted by several different cloud-based storage services. One of the storage services used by Bulletin Board A's members, hereafter referred to as FSS ("File Sharing Site"), offered users free cloud storage for data, documents, images and music. FSS users may store files on the FSS, allow other users to access and download those files, and create passwords to protect their files from download by individuals who do not possess the password.

Based upon the information detailed above, law enforcement had reason to believe that FSS' service was used by members of Bulletin Board A to store files containing child pornography and to make them available to other members. FSS provided this service using computer servers owned, maintained, controlled or operated by a provider whose name is known to law enforcement. The investigation revealed that this provider's headquarters were located in the United States.

On December 7, 2015, the United States District Court of the District of Columbia issued an Order pursuant to 18 U.S.C. § 2703(d), directing FSS to disclose certain records and other information relating to a list of unique URLs that contained files which had been viewed by law enforcement and determined that each depicted minors engaging in sexually explicit conduct.

This Order was sent to FSS. In response to that Order, FSS produced business records which included the dates, times and IP addresses connected to the downloading of the file content associated with the URLs specified in the application for the Order.

FSS provided the following information concerning the access, download and/or attempted download of file content associated with the following unique URL http://[FSS].com/mkj6j8qjxixb/myuimy5r6yu5e433e.7z.html: On October 28, 2015, at 5:51:47 PM (17:51:47) Eastern Daylight Time [EDT], IP address 70.161.118.157 was used to download, and/or attempted to download, file content associated with that URL. That URL contained the link to the above-described 49 second video file depicting what appears to be an adult male from the waist down, with his pants pulled down and with an erect penis, and the lower back and buttocks of what appears to be a minor, engaging in sexual intercourse (either actual or simulated) until the adult male ejaculates on the apparent minor's back and buttocks.

III. The Identification of Defendant's Residence and Execution of the Search Warrant

Using publically available search tools, law enforcement determined that IP address 70.161.118.157 was controlled by Internet Service Provider (ISP[9]) Cox Communications, Inc. (Cox) on the date and time in question. On or about December 15, 2015, a Department of Justice subpoena was issued to Cox requesting subscriber information relating to the use of IP address on October 28, 2015 at 17:51:47 EDT. On or about January 6, 2016, Cox produced

[9] "ISP" refers to the term "Internet Service Provider." Individuals who have an Internet account and an Internet-based electronic mail (e-mail) address must have a subscription, membership, or affiliation with an organization or commercial service which provides access to the Internet. A provider of Internet access and services is referred to as an Internet Service Provider or "ISP."

business records that provided that the account holder, the wife of REECE, was receiving Internet service at defendant REECE's residence (the subject premises) in Chesapeake, Virginia. HSI performed additional public records checks and surveillance, which confirmed that REECE's wife and the defendant REECE, appeared to reside at the subject premises.

On April 5, 2016, a special agent with HSI applied for and was granted a search warrant of the subject premises by this Court. The Honorable Magistrate Judge Lawrence R. Leonard reviewed the application, affidavit in support, and search warrant and signed the search warrant at approximately 2:54 P.M. See Exs. A (Search Warrant), B (Application in Support) and C (Affidavit in Support).

The affidavit in support of the application for the search warrant was written by a HSI special agent who has worked with HSI for almost 10 years. Ex. C, ¶ 1. He is a computer forensic specialist as well as an agent. *Id.* And, he has investigated the sexual exploitation of children for years. *Id.* In his affidavit, the special agent explained the importance and specialization of search and seizing computers and electronic media in appropriate, controlled environments. *Id.* at ¶¶ 27-30. He also discusses the characteristics of those who use the Internet to gain access to child pornography. *Id.* at ¶ 31.

The affidavit also described, in great detail and in stark terms, the purpose of Bulletin Board A. Bulletin Board A was "dedicated to the advertisement, distribution and production of child pornography." Ex. C at ¶ 37. It described the forums and subforums that made it very clear the purpose of Bulletin Board A. *Id*. at ¶ 38. Bulletin Board A's illicit purpose was also apparent to anyone who visited it.

The affidavit also described, in detail, FSS, the third-party file sharing services that hosted some of the files being shared through Bulletin Board A. Ex. C at ¶¶ 37-44. The affiant continued and explained how FSS' responded to a court order with information about the IP addresses that were used to download known images of child pornography from their file sharing service. *Id.* at ¶ 45. He also explained how, on October 28, 2015, the IP address connected to the subject premises was used to download, or at least attempt to download, the described explicit video of the sexual abuse of a child. *Id.* at ¶ 47.

At the time of the application to the search warrant, the affiant had no knowledge if the user of the IP address at the subject premises was indeed a member of Bulletin Board A and he did not state otherwise. The affidavit explained how law enforcement came to believe that a user at the subject premises downloaded child pornography. These URLs were unique and were not searchable. Someone had to share the specific URL and password in order for the user to have accessed it.

The affidavit then explained the link between the IP address and the subject premises. *Id.* at ¶¶ 48-54. Attachments A and B to the search warrant and application in support precisely identified the location to be searched and the items that law enforcement was entitled to seized. Exs. A and C.

The search warrant was executed on April 15, 2016, at the subject premises. Law enforcement seized numerous electronic media. Images of child pornography were located on the electronic media attributable to the defendant.

LEGAL STANDARD & ARGUMENT

An experienced HSI agent explained to a neutral and detached magistrate why there was probable cause to believe that a user who downloaded a video of child pornography approximately five months prior to search warrant application was located at the subject premises. He supported this conclusion with a detailed description of how law enforcement discovered the file sharing service's unique URLs that contained the child pornography. The agent also described how, based on his experience and that of others he spoke with, those that collected child pornography using the Internet and computers had unique characteristics.

Relying on this information, the magistrate judge authorized the HSI to execute a search of REECE's residence. The warrant was a clear in its description of where and what would be searched. The Fourth Amendment asks no more.

As detailed below, nothing in the defendant's First Motion to Suppress undermines this conclusion. There was no "sleight of hand," as the defendant maligns, and no trickery in order to get the search warrant approved by the Court. Defendants seeking the extraordinary remedy of suppression must clear a high hurdle. The defendant falls far short, and his motion should be denied.

I. The warrant affidavit amply supports the magistrate's finding of probable cause for issuance of the warrant

Probable cause exists when "the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found." *Ornelas v. United States*, 517 U.S. 690, 696 (1996). It is a fluid concept that focuses on "the factual and practical considerations of everyday life on which reasonable and prudent men, not

legal technicians, act." *Illinois v. Gates*, 462 U.S. 213, 231 (1983) (internal quotation marks omitted).

Importantly, probable cause does not require a showing of "absolute certainty." *United States v. Gary*, 528 F.3d 324, 327 (4th Cir. 2008). It demands only "a fair probability that contraband or evidence of a crime will be found in a particular place," *Id.* (quoting *Gates*, 462 U.S. at 238), a finding that, in turn, "depends on the totality of the circumstances and involves a 'practical common-sense decision whether'" such a fair probability exists. *United States v. Moses*, 540 F.3d 263, 268 (4th Cir. 2008) (quoting *Gates*, 462 U.S. at 238). "This standard is not defined by bright lines and rigid boundaries." *United States v. Grossman*, 400 F.3d 212, 217 (4th Cir. 2005). "Instead, the standard allows a magistrate judge to review the facts and circumstances as a whole…" *Id.* (citing *United States v. Williams*, 974 F.2d 480, 481 (4th Cir. 1992)). As in this case, "the nature of the unlawful activity alleged, the length of the activity, and the nature of the property to be seized" must be assessed to determine probable cause. *United States v. Richardson*, 607 F.3d 357, 370 (4th Cir. 2010). Further, it is "no defense that the affidavit contained only one allegation or a prior transmission of only one illicit image. Given the evident difficulty of obtaining child pornography, it is very unlikely that an individual would acquire a single image mistakenly or on a whim." *United States v. Ramsburg*, 114 Fed. App'x 78 at *4 (4th Cir. 2004).

Recognizing that reasonable minds may differ regarding whether a particular affidavit establishes probable cause, the Supreme Court "concluded that the preference for warrants is most appropriately effectuated by according 'great deference' to a magistrate's determination." *United States v. Leon*, 468 U.S. 897, 914 (1984) (quoting *Spinelli v. United States*, 393 U.S. 410,

419 (1969); *see also Grossman*, 400 F.3d at 217; *United States v. Blackwood*, 913 F.2d 139,142 (4th Cir. 1990). "[T]he task of a reviewing court is not to conduct a *de novo* determination of probable cause, but only to determine whether there is substantial evidence in the record supporting the magistrate's decision to issue the warrant." *Massachusetts v. Upton*, 466 U.S. 727, 728 (1984). "When reviewing the probable cause supporting a warrant, a reviewing court must consider only the information presented to the magistrate who issued the warrant." *United States v. Wilhelm*, 80 F.3d 116, 118 (4th Cir. 1996) (citing *Blackwood*, 913 F.2d at 142).

The warrant affidavit amply supported a finding of probable cause. The affiant had specialized training and experience in the field, consulted with others who had even more experience than he, and set forth in detail why there was probable cause to believe anyone who downloaded the unique URL from the FSS did so intending to view and/or trade child pornography. Accordingly, his affidavit provided ample justification for obtaining a search warrant and the nexus between the nature of the crime, the facts and circumstance of the crime, and the place to be searched.

Here, the affiant's assessment—and the magistrate's reasonable reliance upon it—was supported by specific, articulable facts and inferences drawn from his training, experience, and that of others. The affiant did not state and did not mislead the Court by stating that REECE was a member of Bulletin Board A. Rather, he explained how the URLs were located, because they were not able to located through search engines or other ways. At most, there was a reasonable inference that the user of the computer may have learned of the URL from Bulletin Board A. These URLs and the files that were contained therein had passwords and were secure. They had to be cut and pasted in order to be shared with others. Indeed, this did not guarantee

that child pornography would be found at REECE's residence. However, the Fourth Amendment requires probable cause only.

Further, the "collector language" used by affiant in the affidavit clearly applies to those that collect child pornography using hidden networks and third-party sites. Law enforcement officers may "draw on their own experience and specialized training to make inferences from and deductions about the cumulative information available to them that might well elude an untrained person." *United States v. Johnson*, 599 F.3d 339, 343 (4th Cir. 2010) (quoting *United States v. Arvizu*, 534 U.S. 266, 273 (2002) (collecting cases). In making probable cause determination, magistrates "may rely upon an experienced officer's conclusions as to the likelihood that evidence exists and where it is located." *United States v. Brown*, 958 F.2d 369 (4th Cir. 1992) (unpublished table decision) (collecting cases); *see also United States v. Terry*, 911 F.2d 272, 275 (9th Cir. 1990) (quoting *United States v. Fannin*, 817 F.2d 1379, 1382 (9th Cir. 1987)); *United States v. Fauntleroy*, 800 F. Supp. 2d 676, 686 (D.Md. 2011) ("The issuing judge is entitled to rely on the affiant's training and experience on the issue whether those involved in certain types of illegality customarily store evidence in their home."). This applies with equal force in child pornography cases. *See, e.g., Richardson*, 607 F.3d at 370-71 (finding affidavit that included statements based on affiant's training and experience regarding child pornography trafficking and storage provided substantial basis for probable cause determination); *United States v. Hay*, 231 F.3d 630, 635-36 (9th Cir. 2000) (same). The defendant is certainly free to disagree with the affiant's assessment, but his disagreement does not mean that the magistrate was compelled to do the same.

II. The probable cause was not stale with a mere five months having passed between the activity and the application for the warrant.

Next, defendant claims that the information contained in the warrant was too stale to support probable cause. The activity traced to REECE's house occurred on October 28, 2015, and the search warrant was signed on April 5, 2016. Approximately five months passed between the alleged criminal activity and the signing of the warrant. Contrary to defendant's assertion, the delay between the download, identification, and the search warrant was not unreasonable and did not hamper the probable cause that was the basis for the search warrant.

A search warrant must allege facts "so closely related to the time of the issue of the warrant as to justify a finding of probable time at that time." *United States v. McCall*, 740 F.2d 1331, 1335-36 (4th Cir. 1984). However, "'[t]he vitality of probable cause cannot be quantified by simply counting the number of days between the occurrence of the facts supplied and the issuance of the affidavit.'" *Id.* at 1336. Instead, as the defendant points out in his memorandum, the Court "look[s] to all the facts and circumstances of the case, including the nature of the unlawful activity alleged, the length of the activity, and the nature of the property to be seized." *Richardson*, 607 F.3d at 370 (quoting *McCall*). Further, findings of staleness "become less appropriate when the instrumentalities of the alleged illegality tend to be retained." *United States v. Ramsburg*, 114 Fed. App'x 78, at *4 (4th Cir. 2004).

In the context of child pornography cases, it is the "widespread view" of courts that "collectors and distributors of child pornography value their sexually explicit materials highly, 'rarely if ever' dispose of such material, and store it 'for long periods' in a secure place, typically in their homes." *Richardson* at 370 (quoting *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997))(four month time period between transmission of child pornography and search warrant

"does not preclude a finding of probable cause based on staleness in light of the other information supplied by" law enforcement); *see also United States v. Sassani*, 139 F.3d 895 (4th Cir. 1998)(upholding a search warrant based on a six month lapse); *United States v. Watzman*, 486 F.3d 1004, 1009 (7th Cir. 2007)("'[i]nformation a year old is not necessarily stale as a matter of law, especially where child pornography is concerned.'")(quoting *United States v. Newsom*, 402 F.3d 780, 783 (7th Cir. 2005)); *United States v. Wagers*, 452 F.3d 534, 540 (6th Cir. 2006); *United States v. Shields*, 458 F.3d 269, 279 n.7 (3d Cir. 2006) (information nine months old not stale); *United States v. Hay*, 231 F.3d 630, 636 (9th Cir. 2000) (six month time period between transmission of child pornography images and warrant did not render information too stale). The Fourth Circuit has gone so far as to say that "information a year old is not stale as a matter of law in child pornography cases." *United States v. Davis*, 313 Fed. App'x 672, 674 (4th Cir. 2009); *but cf. United States v. Raymonda*, 780 F.3d 105, 116-17 (2d Cir. 2015) (nine-month old information was stale).

The Affidavit for Search Warrant requested the ability to conduct a search because on October 28, 2015, a user of a computer downloaded child pornography from defendant's residence in Chesapeake, Virginia. There was only a 5-month lapse between the illegal activity and the search warrant. Further, defendant was not even identified by Cox until January 2016, when Cox Communications responded that REECE's wife was the customer associated with the IP address and that he still had internet connectivity. Thus, there was only a 3-month lapse between the defendant's identification and the execution of the search warrant. As discussed by the HSI agent in his affidavit, those that use the Internet to collect child pornography typically maintained their collections for a long period of time. Three months is nowhere near the one-

year limit set by the Fourth Circuit as a matter of law. Thus, it was reasonable for the issuing judge to believe that the defendant may still possess images of child pornography at his residence and defendant's Motion to Suppress should be denied on this account as well.

III. REECE has made no showing that justifies a *Franks* hearing, let alone established that the warrant contained a material and intentional or reckless falsehood or omission.

"An accused is generally not entitled to challenge the veracity of a facially valid search warrant affidavit." *United States v. Allen*, 631 F.3d 164, 171 (4th Cir. 2011). "In its decision in *Franks v. Delaware,* however, the Supreme Court carved out a narrow exception to this rule, whereby an accused is entitled to an evidentiary hearing on the veracity of statements in the affidavit." *Id.* (citing *Franks v. Delaware,* 438 U.S. 154, 155–56 (1978)). To be entitled to a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978), a defendant "must make a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit." *Franks*, 438 U.S. at 155-56 (quotations omitted). When a *Franks* hearing is sought based on information omitted from an affidavit, the defendant must show: (1) that the omission is the product of a deliberate falsehood or of a reckless disregard for the truth, and (2) inclusion of the omitted information in the affidavit would defeat probable cause. *United States v. Colkley*, 899 F.2d 297, 301-02 (4th Cir. 1990); *accord United States v. Clenney*, 631 F.3d 658, 664-65 (4th Cir. 2011) (affirming denial of motion for *Franks* hearing based on omissions that were neither "designed to mislead the magistrate" nor "material"). In addition to this substantial preliminary showing, a defendant must also demonstrate that the alleged falsity or omission was material to the probable cause determination. *Franks*, 438 U.S. at 155-56; *accord United States v.*

McKenzie-Gude, 671 F.3d 452, 462 (4th Cir. 2011); *United States v. Cioni*, 649 F.3d 276, 286 (4th Cir. 2011); *Clenney*, 631 F.3d at 663; *and Allen*, 631 F.3d at 171. For materiality, the central question is whether the inclusion in the affidavit of the "deliberately omitted facts" would "defeat the probable cause showing and thus render false the original 'literally true' affidavit." *United States v. Tate*, 524 F.3d 449, 456-57 (4th Cir. 2008). This is so because the purpose of a *Franks* hearing is "to prevent the admission of evidence obtained pursuant to warrants that were issued only because the magistrate was misled into believing that there existed probable cause." *United States v. Friedemann*, 210 F.3d 227, 229 (4th Cir. 2000) (emphasis added).

In the seminal case, *Franks v. Delaware*, the Supreme Court stressed that there is a presumption of validity with respect to a search warrant affidavit. 438 U.S. at 155-56. As such, under *Franks*, conclusory allegations of a defect will not do. *Id.* at 171. Defendants must offer allegations of intentional falsehood accompanied by an offer of proof. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished or their absence satisfactorily explained before a hearing is granted. *Id.; see also United States v. Chandia*, 514 F.3d 365, 373 (4th Cir. 2008). Allegations of negligence or innocent mistake are insufficient. *Franks*, 438 U.S. at 171. In *Franks* and subsequent cases, the Supreme Court was clear that the rule it had announced has "a limited scope," one that places a heavy burden on the defendant. *Id.* at 169; *see also United States v. Jeffus*, 22 F.3d 554, 558 (4th Cir. 1994). A defendant cannot meet that burden through a conclusory argument based on "bare allegations" that fail to make the requisite preliminary substantial showing. *United States v. Chandia*, 514 F.3d 365, 373 (4th Cir. 2008).

Applying these principles, there can be little doubt that the defendant has not made anything resembling a substantial, preliminary showing of an intentional or reckless falsehood or omission. First, his offer of proof hardly suffices. He asserts that REECE's IP address never entered a password in order to download the file from the FSS. The government is not clear why REECE believes that a password was needed to download the URL. The password was to open the file, not to download it. The affiant could not and did not swear that the file was ever opened; to wit, he specifically states that the person did or attempted to download the file. This alleged "omission" is not factually correct.

Second, REECE alleges the collector language included in the affidavit was put in without any evidence supporting that REECE was indeed a collector. To the contrary, based on the investigation of a bulletin board hosted on an anonymous network and password protected files on a third-party file sharing service, there was sufficient evidence, in the affiant's experience and in that of others, that the person downloading child pornography through this medium and format could have fit the collector profile.

Third, defendant alleges that the information concerning Bulletin Board A had no nexus to REECE and his residence. Because of the hidden nature of Bulletin Board A, defendant is correct that law enforcement did not know without a doubt that REECE was a member of Bulletin Board A. And, the affiant did not state that REECE was a member of the bulletin board. However, law enforcement's information and belief from their investigation was that only those accessing Bulletin Board A would have access to the unique URLs and passwords containing the child pornography. There was no intentional "hide the ball" or other sinister

plan by law enforcement in its application of the search warrant. It was only based on fact, training, and experience.

Finally, in its conclusion, the affiant concluded that a user at the subject premises received or attempted to receive, possessed and/or accessed with intent to view child pornography "via the listed e-mail account." Ex. C at ¶ 55. Admittedly, this was a typo on behalf of the affiant and in no other place in the affidavit is an "e-mail account" allegedly connected to REECE's residence. However, this was an innocent mistake and not done with malice or otherwise. If a failing at all, it was—at worst—an unintentional oversight. Indeed, it would be a stretch to characterize the agent as negligent; it certainly cannot be said he acted recklessly or with some intent to deceive. And, "mere[ ] negligen[ce] in... recording the facts relevant to a probable-cause determination" is not enough to warrant a *Franks* hearing. *Colkley*, 899 F.2d at 301 (quoting *Franks*, 438 U.S. at 170). Similarly, a "good faith mistake" by the affiant will not invalidate the warrant. *See Id.*

Indeed, much of what he characterizes as "false statement" and "misleading statements" reflect little more than REECE's opinion about the weight the Court should attach to particular statements in the affidavit and the training and experience of those involved with the investigation. The defendant's mere disagreement with the affiant's description of the facts or the inferences to be drawn from those facts in light of his training and experience, however, does not an omission or falsehood make.

The defendant is certainly free to contest whether the facts contained in the affidavit, considering the totality of the circumstances, supported probable cause—as he apparently does. He is not, however, entitled to a *Franks* hearing simply because he does not like the inferences

drawn from those facts by the affiant. And he certainly cannot convert his disagreement into a showing that the affidavit was somehow misleading just by declaring it so. Nothing in *Franks* requires an affiant to "list every conceivable conclusion" and his failure to do so in no way "taint[s] the validity of the affidavit." *Colkley*, 899 F.2d at 301 (quoting *United States v. Burnes,* 816 F.2d 1354, 1358 (9th Cir. 1987)) (internal quotation marks omitted).

Even so, beyond conclusory assertions that a particular statement is wrong or misleading, the defendant offers nothing that would suggest it constitutes an intentional or reckless falsehood. "*Franks* clearly requires defendants to allege more than 'intentional' omission in this weak sense." *Colkley*, 899 F.2d at 301. "To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine." *Franks*, 438 U.S. at 171.

In short, the sum total of the defendant's *Franks* argument seems little more than a recitation of his principal argument against the finding of probable cause: that is, it was theoretically possible that a user may have accessed the URLs without intent to view child pornography. The affiant did not claim otherwise. He merely concluded, based upon the available facts and his training and experience, that it was probably done purposefully and intentionally. More importantly, the magistrate agreed.

IV. None of REECE's claimed defects in the warrant justify the extraordinary remedy of suppression and, even if that warrant does not satisfy the Fourth Amendment, the good faith exception bars suppression.

As a threshold matter, the defendant's dissatisfaction with having been discovered is understandable. But the mere fact that he objects to having been unmasked, without more, does not warrant suppression of evidence obtained pursuant to a warrant issued by a neutral and

detached magistrate based on a finding of probable cause. For all of the reasons outlined above, the warrant does not contravene the requirements of the Fourth Amendment. But even if it did, suppression of the information derived from the execution of that warrant is not appropriate.

The Fourth Amendment's exclusionary rule does not provide "a personal constitutional right, nor is it designed to redress the injury occasioned by an unconstitutional search." *Davis v. United States*, 564 U.S. 229, 236 (2011) (quoting *Stone v. Powell*, 428 U.S. 465, 468 (1976)) (internal quotation marks omitted). The exclusionary "rule's sole purpose … is to deter future Fourth Amendment violations." *Davis*, 564 U.S. at 236 (collecting cases). The real deterrent value "is a 'necessary condition for exclusion,' but it is not a 'sufficient' one." *Id.* at 237 (quoting *Hudson v. Michigan*, 547 U.S. 586, 596 (2006)). There are substantial costs associated with its application. *Id.* ("Exclusion exacts a heavy toll on both the judicial system and society at large…It almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence."). The practical effect in nearly every case "is to suppress the truth and set the criminal loose in the community without punishment." *Id.* (citing *Herring v. United States*, 555 U.S. 135, 141 (2009)). Accordingly, it is to be employed "only as a 'last resort'"—that is, when "the deterrence benefits of suppression … outweigh its heavy costs." *Id.* (quoting *Hudson*, 547 U.S. at 591); *United States v. Stephens*, 764 F.3d 327, 335 (4th Cir. 2014) ("[E]xclusion of evidence has 'always been [the] last resort, not [the] first impulse.'" (quoting *Hudson*, 547 U.S. at 591) (alterations in original)). "Police practices trigger the harsh sanction of exclusion only when they are deliberate enough to yield meaningful deterrence, and culpable enough to be worth the price paid by the justice system." *Id.* (quoting *Davis*, 564 U.S. at 240).

Under the good faith exception to the Fourth Amendment's exclusionary rule, suppression is not warranted when officers rely in good faith on an objectively reasonable search warrant issued by a neutral and detached judge. *United States v. Leon*, 468 U.S. 897, 900 (1984). This objective standard is measured by "whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *Id.* at 922 n. 23. "[A] warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search." *Id.* at 922 (internal quotation marks omitted). The Supreme Court observed that "suppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of the exclusionary rule." *Id.* at 918. The Court identified only four circumstances in which exclusion of evidence seized pursuant to a warrant is appropriate. Those are when: (1) the issuing magistrate was misled by the inclusion of knowing or recklessly false information; (2) the issuing magistrate wholly abandoned the detached and neutral judicial role; (3) the warrant is facially deficient as to its description of the place to be searched or the things to be seized; or (4) the affidavit upon which the warrant is based is so lacking in indicia of probable cause that no reasonable officer could rely on it in good faith. *Id.* at 923-924. None apply here.

Here, the warrant affidavit contained no knowingly or recklessly false information that was material to the issue of probable cause. Nor does the defendant allege that the issuing magistrate abandoned his judicial role. The warrant clearly and particularly described the locations to be searched and the items to be seized. And the affidavit made a strong, comprehensive showing of probable cause to issue the search warrant. Absent any of these

errors, once the magistrate signed the warrant, the agents' reliance on that authority was objectively reasonable. *See Massachusetts v. Sheppard*, 468 U.S. 981, 989-90 (1984) ("[W]e refuse to rule that an officer is required to disbelieve a judge who has just advised him, by word and by action, that the warrant he possesses authorizes him to conduct the search he has requested."). Ultimately, agents acted reasonably in relying on the magistrate's authorization of the warrant, and so the evidence seized pursuant to it should not be suppressed.

CONCLUSION

For the foregoing reasons, the defendant's First Motion to Suppress the search warrant of his residence should be denied.

Respectfully submitted,

DANA J. BOENTE
UNITED STATES ATTORNEY

By:_____/s/_____
Elizabeth M. Yusi
Assistant United States Attorney
Attorney for the United States
United States Attorney's Office
101 West Main Street, Suite 8000
Norfolk, Virginia 23510
Phone: (757) 441-6331
Fax: (757) 441-6678
Email: elizabeth.yusi@usdoj.gov

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 14th day of November, 2016, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send an electronic notification of such filing to the following:

Amanda Conner, Esq.
Kirsten Kmet, Esq.
Assistant Federal Public Defenders

_____/s/_____
Elizabeth M. Yusi
Assistant United States Attorney
Attorney for the United States
United States Attorney's Office
101 West Main Street, Suite 8000
Norfolk, Virginia 23510
Phone: (757) 441-6331
Fax: (757) 441-6678
Email: elizabeth.yusi@usdoj.gov